UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER AUTHORIZING THE RELEASE OF PROSPECTIVE CELL SITE INFORMATION	**Misc. No. 05-508 (JMF)** **UNDER SEAL**

MEMORANDUM

The government once again seeks an order that would require a cell phone company to provide it with "the location of cell site/sector (physical address) at call origination (for outbound calling), call termination (for incoming calls) and, if reasonably available, during the progress of a call, on a real time basis." Proposed Order at ¶ 2.[1] It claims entitlement to the order on the ground that there is "reasonable cause to believe that the requested prospective cell site information is relevant and material to a criminal investigation." Application at 10-11.

There are three standards that might pertain to the government's application: (1) the government may secure a pen register upon the certification that the information sought to be captured by the device is relevant to a criminal investigation (18 U.S. C. § 3122(a)(2)[2]); (2) the government may secure the "contents of wire or electronic communications in a remote computing device" (18 U.S.C. § 2703(b)) or "records concerning electronic communication or remote computing service" (18 U.S.C. § 2703(c)) by (*inter alia*) securing a court order upon a

[1] I granted the government authority to install a pen register on the subject phone in an earlier order.

[2] Note that all references to the United States Code in this document are to the electronic version that appears in Westlaw or Lexis.

showing of specific and articulable facts that the information sought is relevant to and material to an ongoing criminal investigation (18 U.S.C. § 2703(d)); and (3) the government may secure a warrant pursuant to Rule 41 of the Federal Rules of Criminal Procedure upon a showing, consistent with the requirements of the Fourth Amendment, that there is probable cause to believe that what is to be seized is (*inter alia*) evidence of a crime.

As I indicated in my prior opinion, the government's approach melds several of these standards. It states that, while it persists in its view that the government may secure cell site information pursuant to a combination of the Pen Register statute, 18 U.S.C. § 3123, and the Stored Communications Act, 18 U.S.C. § 2703(c), "out of an abundance of caution, pursuant to the Texas Op. and the New York Op. sets forth facts demonstrating probable cause to believe that the requested prospective cell site information is relevant and material to an ongoing criminal investigation." Application at 9-10. In addition, in what the government calls "a further act of caution" (id. at 11), it submits an affidavit prepared by the investigation agent. In that affidavit the agent specifies the information that led him to believe that a person, who we can call "John Doe," is distributing drugs, that he traveled to a certain state to meet with his supply source, and that he used the cell phones at issue to conduct his drug business. The agent therefore concludes that his learning of what he calls "cellular site locations" will provide "evidence of the traveling to the source of supply, locations of stash sites, and distribution of illegal narcotics." Affidavit of Investigating Agent at ¶ 16.

The government's approach puts us back to where we started. The order the government asks me to sign contains my finding that the certification by the Assistant that the information sought to be obtained by the pen register and the affidavit of the agent "support probable cause to

believe that the information sought is relevant" to that investigation and is evidence of "ongoing criminal activity." If one accepts, as I do, that, as three magistrate judges have held,[3] the information the government seeks can only be secured by a warrant issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure, the standard that pertains to the issuance is, as the Fourth Amendment requires, probable cause to believe that the information sought is itself evidence of a crime, not that the information is relevant to an investigation.

The government counters that surveillance of its subject can be expected to produce admissible evidence because the government's knowledge of where he is every moment of the day can be used, as it has been used in reported cases, as evidence that, for example, might rebut an alibi or deny the defendant the ability to say that he was or was not at a certain place. That is certainly true. But, that the information sought might be evidence does not modify the standard guiding whether it can be secured by the means chosen. The government's invocation of an ersatz standard ("probable cause to show relevance to an ongoing investigation") and meeting it cannot overcome my objection to the order it proposes.

The government acknowledges that two opinions[4] of magistrate judges "have suggested that the government must demonstrate probable cause [to believe that that the information sought is evidence of a crime] to obtain disclosure of prospective cell site information." Application at

---

[3] In re: Application for Pen Register and Trap/Device with Cell Site Location Authority, 2005 WL 2656621 (S.D. Tx. Oct. 14, 2005) (hereafter "the Texas Opinion"); In re: Authorizing the Use of a Pen Register, 384 F. Supp. 2d 562 (E.D.N.Y. 2005); In re: Application Authorizing the Use of a Pen Register, 2005 WL 3160860 (D. Md. Nov. 29, 2005).

[4] In fact there are three.

9. It also points to a more recent opinion[5] that suggests that the "reasonable cause standard is the correct one to be met in an application for prospective cell site information." Application at 9.

It must first be noted that the author of the opinion upon which the government relies said nothing about any "reasonable cause" standard. He granted the application upon the certification by the government pursuant to the Pen Register statute that the information was "relevant and material to an ongoing investigation." New York II, 2005 WL 3471754 at *3. Furthermore, the author of that opinion, Judge Gorenstein, could not have been more careful in distinguishing the situation before him from the situations in the three other cases. He indicated that the government was seeking "cell-site information concerning the physical location of the antenna towers associated with the beginning and termination of calls to and from a particular cellphone." Id. at *2. That information permitted the government to "obtain a list of each call made by the subject cell phone, along with a date, start time and end time." Id. Judge Gorenstein then explained the difference between the application made to him and the applications made in the three other cases, decided by magistrate judges:

> The Court is aware of three cases that have considered the availability of cell site data: In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority, 396 F.Supp.2d 747 (S.D.Tex.2005)("Texas Decision") In the Matter of an Application of the United States for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device and (2) Authorizing Release of Subscriber Information and/or Cell Site Information, 396 F.Supp.2d 294 (E.D.N.Y.2005) ("EDNY Decision); and In re Application of the United States for an Order Authorizing the Installation and Use of a Pen Register and a Caller Identification System on Telephone Numbers (Sealed) and Production of Real Time Cell Site Information, 2005 WL 3160860

[5] In re: Application for Disclosure of Telecommunications Records, 2005 WL 3471754 (S.D.N.Y. Dec 20, 2005) (hereafter "New York II").

> (D.Md. Nov.29, 2005) ("Maryland Decision"). These cases appear to involve requests for cell site information that go beyond both what has been sought in this case and what has actually been received by the Government pursuant to any cell site application in this District. First, the cell site information provided in this District is tied only to telephone calls actually made or received by the telephone user. Thus, no data is provided as to the location of the cell phone when no call is in progress. Second, at any given moment, data is provided only as to a single cell tower with which the cell phone is communicating. Thus, no data is provided that could be "triangulated" to permit the precise location of the cell phone user. Third, the data is not obtained by the Government directly but is instead transmitted from the provider digitally to a computer maintained by the Government. That is, the provider transmits to the Government the cell site data that is stored in the provider's system. The Government then uses a software program to translate that data into a usable spreadsheet.

2005 WL 3471754 at *2. Thus, the government misunderstands Judge Gorenstein's holding and then mistakenly claims that it applies to its application in this case even though its application is different from the one Judge Gorenstein approved.[6]

The government also argues that, if the three opinions by magistrate judges denying similar applications are correct, there would be no mechanism by which to "get cell site data whatsoever, which directly contradicts the full intent of Congress expressed in the legislative history and the plain language of 47 U.S.C. § 1002." Application at 9.

The government's reliance on 47 U.S.C. § 1002 is curious because that provision *prohibits* the use of pen registers and trap and trace devices to disclose the location of the person using the phone. That provision requires telecommunication carriers to have the ability to provide "call setup information" to law enforcement agencies. Specifically, 47 U.S.C. § 1002

[6] Note the pains Judge Gorenstein took to warn the government that if it sought any greater information than he was permitting he would require supplemental briefing. New York II, 2005 WL 3471754 at *11.

"requires telecommunications carriers to insure that their equipment is capable of providing a law enforcement agency with information to which it may be entitled under statutes relating to electronic surveillance." New York II, 2005 WL 3471754 at *4. The provision's legislative history indicates that then FBI Director Louis Freech spoke to what he thought was the illegitimate concern that legislation requiring telecommunications carriers to provide what the Director called "call setup information" would permit the tracking of persons. In the subdivision of his statement that he subtitled "Allegations of Tracking Persons," the Director stated:

> Allegations of "tracking" persons
>
> Law enforcement's requirements set forth in the proposed legislation include an ability to acquire "call setup information." This information relates to dialing type information -- information generated by a caller which identifies the origin, duration, and destination of a wire or electronic communication, the telephone number or similar communication address. Such information is critical to law enforcement and, historically, has been acquired through use of pen register or trap and trace devices pursuant to court order.
>
> Several privacy-based spokespersons have criticized the wording of the definition regarding this long-standing requirement, alleging that the government is seeking a new, pervasive, automated "tracking" capability. Such allegations are completely wrong.
>
> Some cellular carriers do acquire information relating to the general location of a cellular telephone for call distribution analysis purposes. However, this information is not the specific type of information obtained from "true" tracking devices, which can require a warrant or court order when used to track within a private location not open to public view. See United states v.Karo, 468 U.S. 705, 714 (1984). Even when such generalized location information, or any other type of "transactional" information, is obtained from communications service providers, court orders or subpoenas are required and are obtained.
>
> In order to make clear that the acquisition of such information

> is not being sought through the use of a pen register or trap and trace device, and is not included within the term "call setup information," we are prepared to add a concluding phrase to this definition to explicitly clarify the point: except that such information (call setup information) shall not include any information that may disclose the physical location of a mobile facility or service beyond that associated with the number's area code or exchange.

Statement of Louis J. Freeh, Director, FBI, Before the Senate Joint Judiciary Technology, Law, Civil and Constitutional Rights at 29 (March 18, 1994) reprinted in Federal Document Clearing House, 1994 WL 223962.

The Director's offer and its acceptance by Congress led to the exception codified as 47 U.S.C. § 1002(a)(2). Thus, the statute enacted to require that telecommunications carriers have certain capabilities provided, as a somewhat grammatically incongruous exception to the imposition of required capabilities, that:

> except that, with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127 of Title 18), such call-identifying information[7] shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number)

47 U.S.C. § 1002(a)(2).

Thus, while the legislation spoke to capabilities, the exception was based on the express

---

[7] The term "call-identifying information" means dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier. 47 U.S.C. § 1001(2).

representation by the government to Congress that the authority for pen registers and trap and trace devices would not and could not be used to secure location information, the very information the government now wants to secure by using a pen register and trap and trace device.

The government does not argue the significance of any legislation enacted since 1994 that would express any intention by Congress to revise or repeal this legislation and, therefore, proposes no reason whatsoever why it is no longer in force and effect. Furthermore, in the Texas Opinion, Judge Smith explains why the Patriot Act's expansion of the definitions in the Pen Register statute cannot possibly be read as granting the government the very authority to use that statute to secure the data the same government assured Congress it could not secure using that statute in 1994. Texas Op., 2005 WL 2656621 at *13-*15.

I appreciate that a fundamental premise of Judge Gorenstein's opinion is that, if the Pen Register statute does not permit the government to use the Pen Register statute to secure cell site information, the information is absolutely unavailable. New York II, 2005 WL 3471754 *4. This conclusion troubles Judge Gorenstein because of indications, contemporaneous to the Congressional consideration of the legislation Director Freeh was proposing, that physical location data would have been obtainable under the Pen Register statute and the exception that I have quoted above would have been unnecessary if the Pen Register statute did not permit the acquisition of physical location data. Id. The judge then reasons that, because the exclusion indicates that what Driector Freeh called "call setup information" and what the exclusion calls

"call-identifying" information that may disclose the location of the subscriber"[8] may not be secured "solely" by a trap and trace device, Congress intended to its being captured by some other means in addition to the trap and trace device. He then finds that a provision in the Stored Communications Act, enacted by another Congress and codified in 18 U.S.C. § 2703, grants that additional means by which the government may install a trap and device and secure the cell site data that would disclose the subscriber's location.

The explicit premise of this analysis is the perception that in 1994 Congress understood that information that disclosed the location of the person using a cell phone could be secured by a trap and trace device and intended that it be secured by some means other than a trap and trace device. I can find no contemporaneous indication that, in 1994, Congress had any such understanding, let alone that it was aware of the technology now available that, by triangulation, permits the government to know where the cell phone is. The converse is true. Congress, at most, understood that a communications provider could acquire what Director Freeh called "information relating to the general location of a cellular telephone" and, at his request, precluded the use of the Pen Register statute to secure it.

We have to begin with the Director's statement quoted above. To rebut the claim that the statute he proposed, by permitting the government to secure "call setup information," would grant the government a "pervasive, automated 'tracking capability,'"[9] he first assured Congress that, while certain carriers "do acquire information relating to the general location of a cellular

---

[8] 47 U.S.C. § 1002(a)(2)

[9] 1994 WL 223962 at *17.

telephone for call distribution analysis purposes," that kind of information was not the kind of information that would or could be obtained by the use of a "true" tracking device, i.e., a device affixed to a car that permitted its movement to be monitored. He than stated that "when such generalized location information" was obtained, it was by the use of court orders and subpoena, meaning that the claim that the authority he sought to secure "call setup information" by the Pen Register was false and he neither could nor wanted to use the Pen Register statute to secure it. While he may have thought it unnecessary, he nevertheless indicated that he would have no objection to Congress insisting that, while a carrier could be required to produce call setup information, it could not be required to disclose any information that might disclose the physical location of a mobile facility or service.

Thus, there is nothing in Freeh's statement suggesting that he had any knowledge of the possibility that a pen register could be used to secure cell site information that disclosed the location of the cell phone user by, for example, the triangulation of contemporaneous transmission from the phone or any other means of capturing the location of the cell phone during the transmission of a call.

The Senate and House reports about the legislation that contained the exception at issue similarly indicate that, at most, Congress was aware, as Freeh was aware, that transactional data about the cell phone might disclose "location information." The House Report stated that the bill Freeh proposed:

> Expressly provides that the authority for pen registers and trap and trace devices cannot be used to obtain tracking and location information, other than that which can be determined from the phone number. Currently, in some cellular systems, transactional data that could be obtained by a pen register may include location

information.

H.R. Rep. No. 103-827(I) (1994), reprinted in 1994 U.S.C.C.A.N. 3489, 3497, available at 1994 WL 557197 at *17.[10] This statement indicates that, at most, the "transactional data maintained" by the carrier might yield information as to where the phone was located once the pen register was installed.

Thus, whatsoever the actual existence of the technology in 1994, I cannot find any contemporaneous understanding by either Director Freeh or the Congress that the government had the capability that it now has to ascertain the location of a person using a cell phone, let alone that Congress intended to permit the government to use the Pen Register statute to avail itself of that technology, provided it combined its use of that statute with some other means. While the government would counter, relying on Judge Gorenstein's opinion, that the word "solely" in 47 U.S.C. § 1002 (a)(2) suggests that this is true because it only precludes use of the Pen Register statute itself, I would have to answer that this conclusion, besides being historically inaccurate, reaches an utterly counter-intuitive conclusion. It is inconceivable to me that the Congress that precluded the use of the Pen Register statute to secure in 1994 "transactional data" or what Freech called "call up information" nevertheless intended to permit the government to use that same statute, whether by itself or combined with some other means, to secure the infinitely more intrusive information about the location of a cell phone every minute of every day that the cell phone was on. I cannot predicate such a counter-intuitive conclusion on the single word "solely."

---

[10] The Senate Report is to the same effect. S. Rep. No. 103-402 (1994), available at 1994 WL 562252 at *18 (1994).

I therefore persist in my view that the government lacks the power to secure the information it seeks and will once again decline to sign the proposed order the government has tendered.

_____

JOHN M. FACCIOLA
UNITED STATES MAGISTRATE JUDGE

Dated: